This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

THIS PAGE BLANK (USPTO)

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/32 | A1

(11) International Publication Number: WO 00/11834

(43) International Publication Date: 2 March 2000 (02.03.00)

(21) International Application Number: PCT/US98/17605

(22) International Filing Date: 25 August 1998 (25.08.98)

(71) Applicant: SCHLUMBERGER INDUSTRIES, S.A. [FR/FR]; 50, avenue Jean-Jaures, F-92120 Montrouge (FR).

(71)(72) Applicant and Inventor: CRONIN, Mary, J. [US/US]; 80 Manemet Road, Newton, MA 02159 (US).

(72) Inventor: GUTHERY, Scott, B.; 19 Foster Road, Belmont, MA 02178 (US).

(74) Agents: SMITH, James, M. et al.; Hamilton, Brook, Smith & Reynolds, P.C., Two Militia Drive, Lexington, MA 02421 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: GRAPHIC DIGITAL SIGNATURES

(57) Abstract

A method for steganographically embedding digital signatures into graphic and audio attachments in electronic communications such as e-mail, World Wide Web pages, etc. Recipients, seeing the graphic or hearing the audio, are made aware of the existence of the embedded digital signature and may request that it be validated. The digital signature is extracted from the attachment and validated for the recipient.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

PNSDOCID: <WO 0011834A1 | >

GRAPHIC DIGITAL SIGNATURES

BACKGROUND OF THE INVENTION

With the increased usage of the Internet and other computer networks, it is becoming increasingly important to be able to ensure that an electronic message received over a network is both authentic, i.e., that the sender is who he claims to be, and that the message has not been altered by some third party en route.

Digital signatures have been developed to fill this need. A digital signature is a digital representation of information identifying the author or source of a document which includes but is not limited to a demonstration of knowledge of secret or little-known information

Generally, a sender, using a computer or similar digital means, composes a message he intends to send to one or more recipients. At the sender's request, or automatically, a digital signature is derived based on some aspect of the message. How the digital signatures are actually coded and decoded are beyond the scope of this patent, but see Mitchell, Piper and Wild, "Digital Signatures", Contemporary Cryptology, pp. 325-378, which is incorporated herein by reference.

Digital signatures are typically attached to digital messages which are passed from one computer to another via a network - from small, in-house intranets to the large networks such as the Internet. Current methods represent digital signatures as large blocks of alphanumeric,

hexadecimal or binary characters. For example, a digital signature might be represented in an electronic mail (e-mail) as follows:

iQBFAgUBM0jm3ygmpqV0uJ6VAQFOqwF/emw7/F1wFFe3q00H1QZbtzJI5Y2
RKMgYovXpsOsUgNVAbqHMiyHD2uTDLVxdID76=THEF

Representations such as this are not only aesthetically unpleasing to a human recipient but due to their highly technical appearance may serve to discourage non-technical users from using digital signature technology altogether.

SUMMARY OF THE INVENTION

Representing digital signatures in meaningful and intuitive graphical and audio forms allows non-technical users to easily understand their purpose. Such users are therefore more likely to use digital signatures. By providing a method for personalizing the display of a digital signature, all users are encouraged to use digital signatures in their own messages.

The present invention provides means for steganographically embedding a digital signature into a more intuitive signature graphic such as is shown at 50 in Fig. 1 or into an audio recording of the sender saying something such as "This document about widget pricing dated May 23, 1997, has been written by me."

In accordance with the present invention, a method of digital communication comprises the steps of providing a digital message that the sender desires to send to one or more recipients; providing a digital signature such as a

private key encrypted hash of the message or a biometric such as a private encryption key or unique biometric information such as a facial picture, a fingerprint, an iris or retinal scan, typing and handwriting patterns, hand or finger geometry or a voice print; providing a user-perceptible attachment such as a picture or audio; embedding the digital signature into the attachment; attaching the attachment to the message to form a digital communication; and sending the communication.

In a preferred embodiment, the digital signature is embedded into the attachment by substituting bits of the digital signature into selected least significant bits of the attachment. In this manner, the changes to the attachment are virtually undetectable by the recipient. The existence or the state of the attachment itself may alert the recipient to the fact that a digital signature is present. Furthermore, a header may be embedded into the attachment at predetermined locations. This header may serve to identify the existence of the digital signature, or the header may contain parameters which provide further information about the digital signature, e.g., coding technique, location within the attachment, etc.

The attachment may be modified before embedding the digital signature by any number and manner of transformations. Such modification may be used to alert the recipient that a digital signature is present. Examples of such modification transformations are warping and morphing.

Either the recipient can initiate verification of the digital signature, or such verification can come about

automatically. Generally, when a communication is received, both the message and the attachment are available to the recipient. The recipient may begin the verification process, for example, by selecting the attachment using a computer mouse. Verification comprises extracting the digital signature from the attachment and verifying the validity of the digital signature according to standard digital signature techniques. Finally, the recipient may be notified as to whether the digital signature is valid or not, or the digital signature may be displayed to the recipient. The software that forms those functions may, for example, be incorporated in otherwise conventional e-mail software.

The above and other features of the invention including various novel details of construction and combinations of parts, and other advantages, will now be more particularly described with reference to the accompanying drawings and pointed out in the claims. It will be understood that the particular method and device embodying the invention are shown by way of illustration and not as a limitation of the invention. The principles and features of this invention may be employed in various and numerous embodiments without departing from the scope of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other objects, features and advantages of the invention will be apparent from the following more particular description of preferred embodiments and the drawings in which like reference characters refer to the same parts throughout the different

views. The drawings are not necessarily to scale, emphasis instead being placed upon illustrating the principals of the invention.

Fig. 1 illustrates a graphic signature as it might appear in an e-mail.

Fig. 2A illustrates a prior art electronic e-mail communication with an alphanumeric representation of a digital signature.

Fig. 2B illustrates an electronic e-mail communication with a graphic in which a digital signature is steganographically embedded.

Fig. 3 is a flowchart showing generally the process of embedding a digital signature.

Fig. 4 is a flowchart showing generally the process of extracting a digital signature and further processing it.

Fig. 5 illustrates a graphic which could be used to notify a recipient of a valid digital signature.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Fig. 2A illustrates an electronic mail (e-mail) communication 100 as it might appear in prior art. The sender has composed a message 102, in this example, consisting of the sentence "Please give Alice Gilbert a master key," followed by a salutation. A digital signature 104 is generated. The digital signature may be based on the message 102 and a key known or provided to the sender's computer, or it may be independent of the message 102 itself, as in the case where the signature is a fingerprint. The digital signature 104 is appended to the message 102, along with some additional information 106, to form the digital communication, which is transmitted or sent to one or more intended recipients. A non-technical

person receiving this message may not immediately know the purpose of the digital signature 104 and/or how to use it.

Fig. 2B illustrates the equivalent email communication 110 as produced by the present invention. A message 112 consists of some text the sender wishes to convey to the recipient, again, in this example, the sentence "Please give Alice Gilbert a master key," followed by a salutation. In this example, however, a graphic, digitized (not digital) signature 114 of the sender (Sally) is attached to the communication. This graphic 114 has been slightly altered such that it contains the same digital signature as shown in 104 of Fig. 2A.

When the signed email 110 of Fig. 2B arrives at its destination and is selected for reading by the recipient, the recipient is offered the opportunity to verify the signature. If the user decides to verify the signature, for example by selecting a "Verify" button, then the e-mail software extracts the digital signature 104 from the graphic 114 and performs the usual digital signature verification. If the digital signature 114 is verified, i.e., the digital signature supports the claim that the email comes from Sally Green, the software might display an acknowledgment such as "Signature verified as the signature of Sally Green," or a graphic 60 such as that shown in Fig. 5.

Of course it would be understood in the art that the message may be text, audio, graphic, or some other mode of conveying information digitally. Furthermore, it would be understood that the communication is not limited to email. For example, the communication could be a transmittal of a

World Wide Web page or some other means of digitally transmitting a message. Finally the attachment into which the digital signature is embedded may itself be text, audio, graphic, video, etc.

The attachment may be modified before embedding the digital signature. For example, warping and morphing, as well as other transformations, may be applied to a graphic or picture. Similarly, other types of transformations may be applied to audio signals. Such modifications may be used to alert the recipient that a digital signature is present.

Fig. 3 is a flowchart showing generally the process of embedding a digital signature. First, at 200, the sender composes or otherwise provides a message comprising the information he wishes to communicate to the recipients. At 202 an image or audio attachment is provided, and at 204 a digital signature is calculated or otherwise provided. Examples of suitable digital signature algorithms can be found in "Digital Signature Schemes" by Birgit Pfitzmann and published by Springer-Verlag in 1996 (ISBN 3-540-61517-2) which is herein incorporated by reference.

The attachment can be modified using image processing or audio processing algorithms. The purpose of this transformation is to provide to the recipient an indicator that a digital signature has been included and can be validated. For example, an image may undergo warping 206, morphing 208, and/or other transformations 210. Audio be may subjected to audio-type transforms, for example, filtering.

Warping 206 is typically applied to line-drawing images and comprises bending or moving some of the lines in the image. For example, if the original attachment is an image of a dragonfly and the body of the dragonfly is a long, curved cigar shape, this image can be warped by increasing or decreasing the bending of the body of the dragonfly. In one embodiment of the present invention, the amount of warping is determined based on parameters computed from the document such as a word count.

Morphing algorithms 208 transform one image to another by computing a series of images visually between a beginning image and an ending image. In one embodiment of the present invention, a user chooses an ending image to morph an original "signing" image toward. If some computed value for the message, such as a word count or a digital signature, is n on a scale from 0 to N, then the image that is n/N of the way from the original signing image to the ending image is selected as the attachment in which the digital signature will be embedded. Examples of suitable warping and morphing algorithms can be found in "Digital Image Warping" by George Wolberg and published by the IEEE Computer Society Press in 1990 (ISBN 0-81868944-7) which is herein incorporated by reference.

Referring again to Fig. 3 after the transformations 206, 208, 210 have been applied to the attachment, the digital signature is embedded into the attachment using steganographic techniques 212, described below. The attachment is attached 214 to the message to form a communication, and finally, the communication is transmitted 216 to the intended recipients.

Steganographic algorithms are typically used to hide information in images, although the technique is easily applied to digital audio signals as well. What appears to be an innocent picture actually contains a secret message. The embedding of the text into the picture is deliberately constructed so as to not disturb the image such that a viewer cannot tell that the picture contains a message simply by looking at it. In other words, the embedding does not alter - at least to the human eye or ear - the appearance of the picture or the sound of an audio. Suppose for example that a black and white photograph exists such that each point (pixel) in the photograph is represented as a 16-bit number where 0 represents all white, 32,768 represents all black and numbers in between represent shades of gray between white and black. Taking a digital signature as a string of bits, the digital signature can be embedded into the photograph by setting the low-order bit of a pixel (a point in the photograph) of the photograph to 0 when the corresponding bit in the digital signature is 0, and to 1 when the corresponding bit in the digital signature is 1. If the low-order bit in the pixel were originally 0 and it is now set to 1, then the pixel becomes just a little darker, but not enough to be noticeable. Similarly, if the low-order bit in the pixel were originally 1 and it is now set to 0, then the pixel becomes just a little brighter, but again not enough to be noticed. Continuing in this fashion, all of the bits of the digital signature can be embedded into the photograph without visually changing it. Examples of suitable steganographic algorithms can be found in "Information Hiding: Proceedings of the First International Workshop, U.K. May 30 - June 1, 1996" edited by Ross Andersion and

published by Springer-Verlag in 1996 (ISBN 3-540-61996-8) which is herein incorporated by reference.

In the present invention, it is not the intention to actually hide the digital signature from a recipient, that is prevent a recipient from accessing the embedded digital signature, but rather to use the attachment to "carry" the digital signature in such manner that the attachment is not noticeably altered by the digital signature.

Fig. 4 is a flowchart showing generally the process of extracting and processing the digital signature from the received communication. First, the communication must be received by the recipient or his computer 302. The recipient must be made aware that the communication contains an embedded digital signature. This is done by displaying 304 the graphic attachment so that the recipient can see it, or, in the case of an audio attachment, playing the attachment so that the recipient hears it. Any transformations which have been applied may themselves be the clue to the recipient that a digital signature has been embedded.

The recipient can then ask for validation of the digital signature 306 and the digital signature is extracted from the attachment 308 by reading the bits known to contain the digital signature. In a preferred embodiment, the digital signature is verified 310 and the recipient is notified 312 as to whether the signature is valid or not. Alternatively, the extracted digital signature can be displayed 314 for the recipient's viewing.

While this invention has been particularly shown and described with references to preferred embodiments thereof, it will be understood by those skilled in the art that various changes in form and detail may be made therein without departing from the spirit and scope of the invention as defined by the appended claims.

CLAIMS

1. A method of digital communication comprising:
providing a digital message;
generating a digital signature related to the message; and
embedding the digital signature in a user-perceptible attachment accompanying the digital message.

2. A method as in Claim 1 wherein embedding the digital signature comprises the steps of:
selecting bits within the attachment;
associating bits of the digital signature with the selected bits; and
altering the selected bits by writing the digital signature bits into the associated attachment bits.

3. A method as in Claim 2 wherein a known header string is inserted at a predetermined location in the attachment.

4. A method as in Claim 3 wherein the header string comprises parameters describing the digital signature.

5. A method as in Claim 1 further comprising the step of modifying the attachment before the step of embedding the digital signature.

6. A method as in Claim 1 wherein the attachment is a digital picture.

7. A method as in Claim 6 wherein the digital picture is a representation of an entity whose identity is being embedded in the picture.

8. A method as in Claim 6 further comprising the step of modifying the digital picture before the step of embedding the digital signature.

9. A method as in Claim 8 wherein the step of modifying the digital picture comprises warping the digital picture according to a computed value.

10. A method as in Claim 9 wherein the computed value is the digital signature.

11. A method as in Claim 8 wherein the step of modifying the digital picture comprises morphing the digital picture according to a computed value.

12. A method as in Claim 1 wherein the attachment is a digitized audio passage.

13. A method as in Claim 12 further comprising the step of modifying the audio passage in accordance with a computed value, before the step of embedding the digital signature.

14. A method as in Claim 12 wherein the audio passage is a voice recording of an entity whose identity is being embedded in the audio passage.

15. A method as in Claim 1 wherein the digital signature is generated from a private encryption key.

16. A method as in Claim 1 wherein the digital signature is a digitized biometric.

17. A method as in Claim 16 wherein the digitized biometric is a digital fingerprint.

18. A method as in Claim 16 wherein the digitized biometric is a digital voiceprint

19. A method as in Claim 16 wherein the digitized biometric is a digital retina scan.

20. A method as in Claim 1 further comprising:

including the attachment with the embedded digital signature in a digital communication;

transmitting the digital communication to a recipient;

receiving the digital communication at the recipient;

extracting the digital signature from the attachment within the received digital communication; and

processing the extracted digital signature.

21. A method as in Claim 20 wherein the step of processing the extracted digital signature comprises:

verifying validity of the digital signature; and

notifying the recipient as to whether the digital signature is valid or not.

22. A method as in Claim 21 further comprising before the step of verifying validity:

providing a means wherein the recipient is made aware of the existence of the digital signature; and

providing a means wherein the recipient can indicate that the digital signature should be validated, at which time the verifying and notifying steps take place.

23. A method as in Claim 21 wherein the step of processing the extracted digital signature comprises:

displaying the digital signature to the recipient.

24. A computer system for sending a digital communication comprising:

means for providing a digital message;

means for generating a digital signature related to the message;

means for embedding the digital signature in a user-perceptible attachment;

means for attaching the attachment to the message to form the digital communication; and

means for sending the communication to a recipient.

25. A computer system for verifying authenticity of a received digital communication comprising:

means for receiving the digital communication comprising a digital message and a user-perceptible attachment;

means for extracting the digital signature from the attachment; and

means for processing the digital signature.

26. A computer system as in Claim 25 wherein the means for processing the digital signature further comprises:

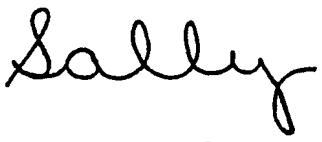
means for verifying validity of the digital signature; and

means for notifying a recipient as to whether the digital signature is valid or not.

27. A computer system as in Claim 25 wherein the means for processing the digital signature further comprises:

means for displaying the digital signature to the recipient.

FIG. 1



50

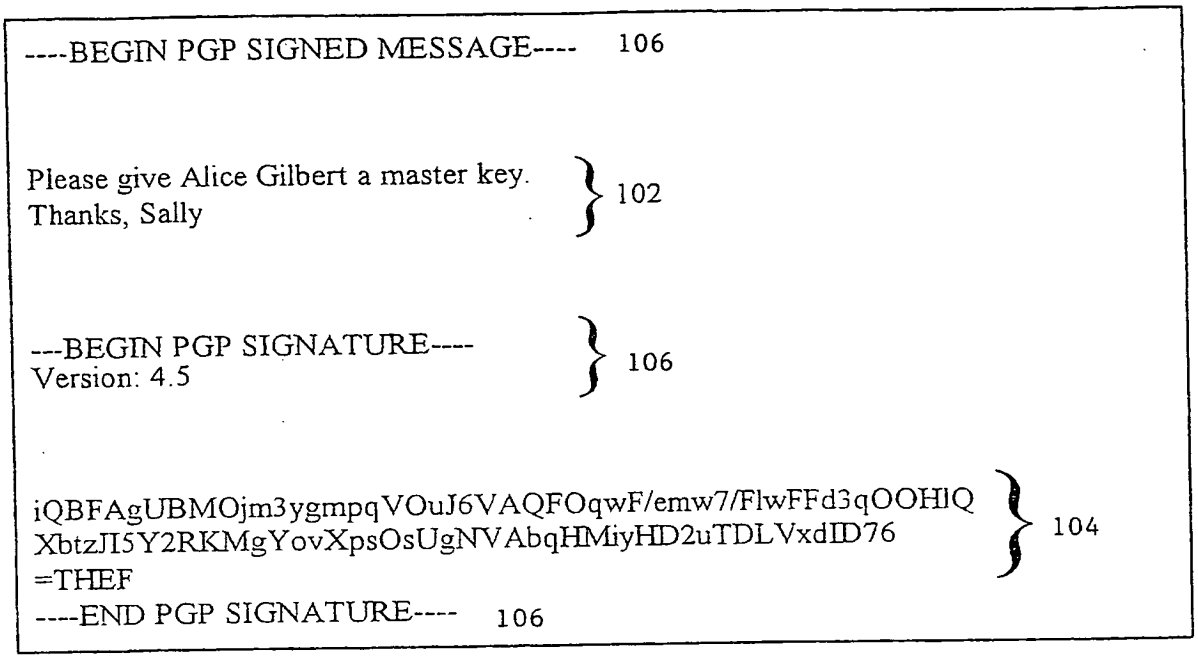


FIG. 2A
(prior art)

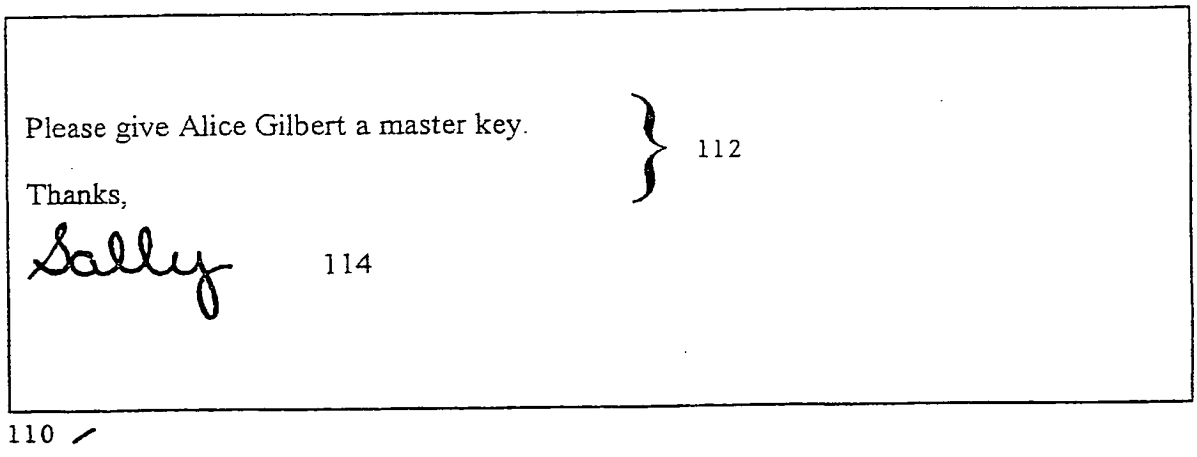


FIG. 2B

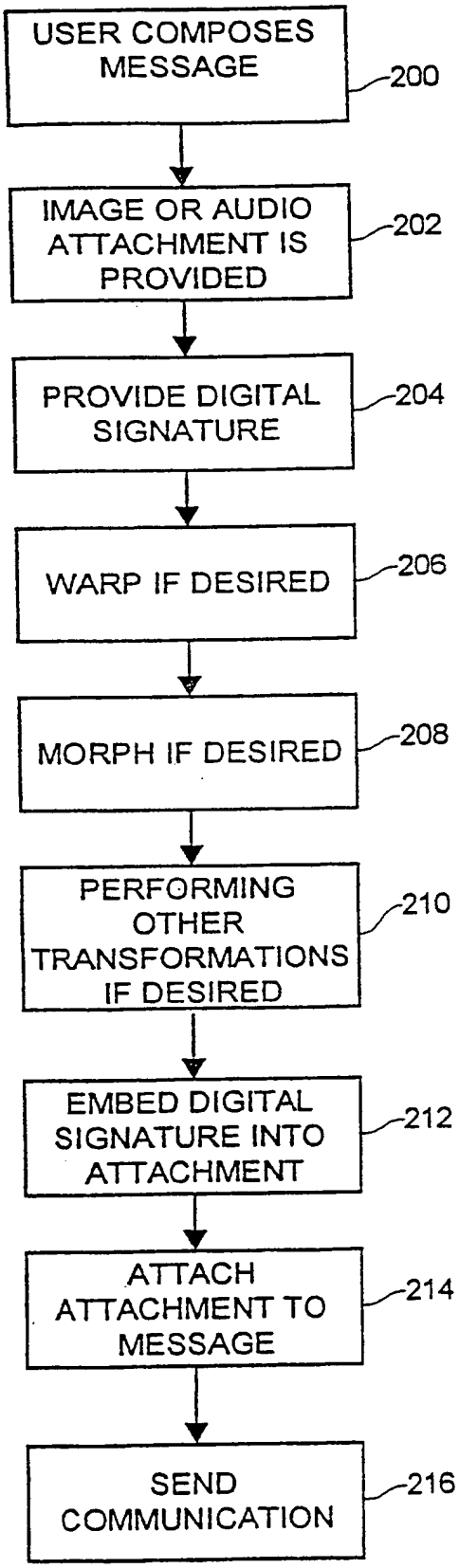

USER COMPOSES MESSAGE
200
IMAGE OR AUDIO ATTACHMENT IS PROVIDED
202
PROVIDE DIGITAL SIGNATURE
204
WARP IF DESIRED
206
MORPH IF DESIRED
208
PERFORMING OTHER TRANSFORMATIONS IF DESIRED
210
EMBED DIGITAL SIGNATURE INTO ATTACHMENT
212
ATTACH ATTACHMENT TO MESSAGE
214
SEND COMMUNICATION
216

FIG. 3

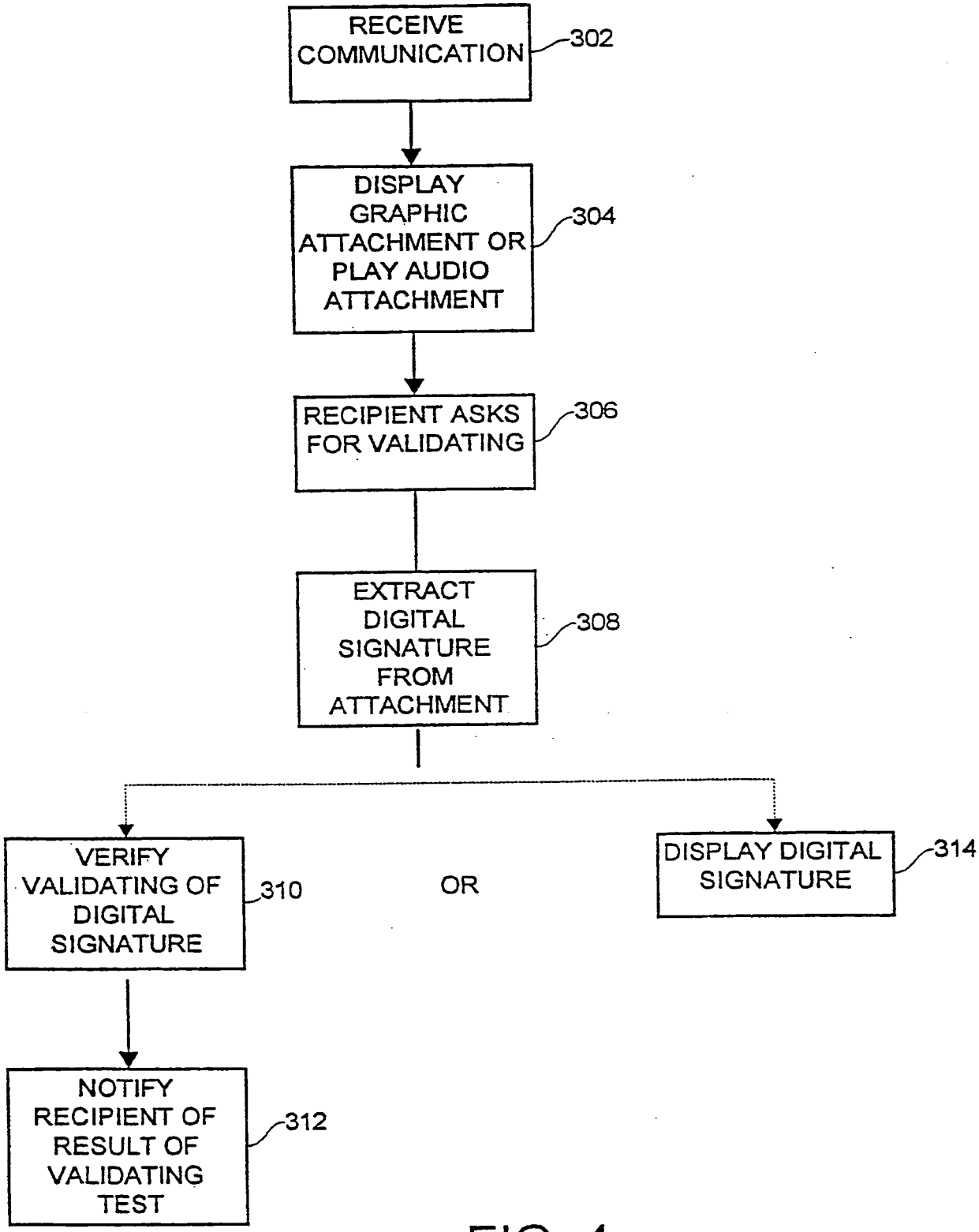
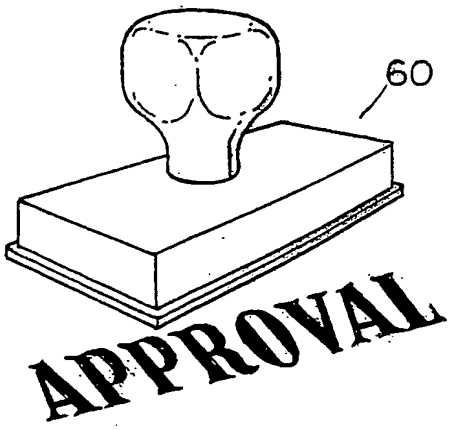

RECEIVE COMMUNICATION
302
DISPLAY GRAPHIC ATTACHMENT OR PLAY AUDIO ATTACHMENT
304
RECIPIENT ASKS FOR VALIDATING
306
EXTRACT DIGITAL SIGNATURE FROM ATTACHMENT
308
VERIFY VALIDATING OF DIGITAL SIGNATURE
310
OR
DISPLAY DIGITAL SIGNATURE
314
NOTIFY RECIPIENT OF RESULT OF VALIDATING TEST
312

FIG. 4

FIG. 5



INTERNATIONAL SEARCH REPORT

Inter. .onal Application No
PCT/US 98/17605

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y A	US 5 765 176 A (BLOOMBERG DAN S) 9 June 1998 see column 14, line 18 - column 15, line 24 see column 22, line 59 - line 63 see column 26, line 65 - column 27, line 45 see figures 17,18 --- -/--	1,2,6-8, 15,25-27 12-14, 16-18 10,20-24

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 April 1999	23/04/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Masche, C

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Intern. .onal Application No
PCT/US 98/17605

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 781 635 A (CHAN KEEN) 14 July 1998	1,6,7, 15,20-27
A	see column 1, line 14 - line 20 see column 2, line 62 - column 3, line 19 see column 5, line 26 - line 30 see column 5, line 45 - line 52 see column 6, line 9 - line 17 see figure 2A	10
Y	WO 96 42151 A (DICE COMPANY) 27 December 1996	12-14
A	see abstract see page 24, line 23 - page 26, line 7	15
Y	DE 42 43 908 A (GAO GES AUTOMATION ORG) 30 June 1994 see abstract see column 2, line 37 - line 43 see column 3, line 47 - column 4, line 13	16-18
A	"AUTHENTICATION AND DISPLAY OF SIGNATURES ON ELECTRONIC DOCUMENTS" RESEARCH DISCLOSURE, no. 358, 1 February 1994, page 75 XP000439803 see the whole document	1,6,15, 20-27
A	EP 0 246 823 A (RACAL GUARDATA LTD) 25 November 1987 see the whole document	1,15, 20-27

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

BNSDOCID: <WO _____0011834A1_I_>

INTERNATIONAL SEARCH REPORT

Information on patent family members

Intern. ɔnal Application No
PCT/US 98/17605

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5765176 A	09-06-1998	NONE	
US 5781635 A	14-07-1998	NONE	
WO 9642151 A	27-12-1996	US 5613004 A	18-03-1997
		EP 0872073 A	21-10-1998
		US 5687236 A	11-11-1997
DE 4243908 A	30-06-1994	NONE	
EP 0246823 A	25-11-1987	AU 590082 B	26-10-1989
		AU 7326487 A	26-11-1987
		GB 2190820 A,B	25-11-1987
		HK 78690 A	12-10-1990
		JP 63010839 A	18-01-1988
		US 4890323 A	26-12-1989

RNSDOCID: <WO 0011834A1 I >